



## **Policies and Procedures**

Subject: Administration of HIPAA

Policy Number: HIPAA 3.2

Effective Date: 12/15/03

Entity Responsible: Division of General Counsel

Revision Date: 1/11/18

### **1. Purpose:**

To provide a process to designate personnel to develop, implement, and administer the Tennessee Department of Mental Health and Substance Abuse Services' (TDMHSAS) policies and procedures that comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, federal law, and Tennessee law.

### **2. Policy:**

- 2.1: The TDMHSAS Commissioner shall designate a HIPAA Compliance Officer (TDMHSAS Privacy Officer) who is responsible for administering, developing, and implementing the policies and procedures of the TDMHSAS to comply with HIPAA rules and regulations, as well as other federal and state privacy laws. This designation must be documented and maintained for six (6) years. The TDMHSAS Privacy Officer shall be a licensed attorney, serving in the Office of General Counsel, TDMHSAS Central Office, and shall be able to understand, interpret, explain, and ensure Departmental compliance with federal and state laws and regulations concerning privacy and security of confidential information.
- 2.2: The TDMHSAS shall designate a contact person who is responsible to document, process, and resolve of HIPAA complaints, who is able to provide information about matters concerning adequate notice of the uses and disclosures of protected health information (PHI). This person shall work to ensure that any person wanting to file a complaint is not intimidated, threatened, coerced, discriminated against, or retaliated against by any member of the TDMHSAS workforce. The

TDMHSAS Privacy Officer, as described in 2.1, shall service as the TDMHSAS contact person discussed in 2.2.

- 2.3: Each Regional Mental Health Institute (RMHI) CEO shall designate a HIPAA Privacy Officer (RMHI Privacy Officer) who is responsible for providing information about the use, disclosure, and safeguarding of PHI at the RMHIs, and who is responsible for the implementation of TDMHSAS' policies and procedures under HIPAA rules and regulations, as well as federal and state privacy laws. This designation must be documented and maintained for six (6) years. The RMHI Privacy Officer will also serve as the contact person for the RMHI to document and process HIPAA complaints.
- 2.4: The TDMHSAS Commissioner shall also designate a HIPAA Security Officer (TDMHSAS Security Officer) who is responsible for implementing the policies and procedures of TDMHSAS to comply with HIPAA security rules and regulations, and who is responsible for preventing, detecting, containing, and correcting HIPAA security violations. This designation must be document and maintained for six (6) years. The TDMHSAS Security Officer must be an information technology and information systems professional who serves the TDMHSAS.
- 2.5: Each RMHI Chief Officer shall designate a HIPAA Security Officer (RMHI Security Officer) who is responsible for implementing the policies and procedures of the TDMHSAS to comply with HIPAA security rules and regulations, and who is responsible for preventing, detecting, containing, and correcting HIPAA security violations. This designation must be documented and maintained for six (6) years.

### **3. Procedure/ Responsibility:**

- 3.1: Duties of the TDMHSAS Privacy Officer:
  - 3.1.1: Develop HIPAA programs, publish and distribute the updated HIPAA privacy notice, maintain HIPAA policies and procedures in written or electronic form.
  - 3.1.2: Ensure that all TDMHSAS HIPAA privacy policies and procedures are accessible to all TDMHSAS and RMHI employees and available to the general public via internet access through the TDMHSAS website. TDMHSAS HIPAA security policies and procedures are accessible to all TDMHSAS and RMHI employees through a shared drive.

- 3.1.3: Monitor compliance with HIPAA rules, regulations, policies, and procedures; require appropriate sanctions against workforce members who fail to comply with privacy policies and procedures; update policies and procedures as necessary.
- 3.1.4: Serve as the designated decision maker for legal issues concerning HIPAA regulations, policies, and procedures, and provide guidance to TDMHSAS executive officers, RMHI attorneys, and the RMHI HIPAA officers described in 2.3 and 2.5 involving interpretation and application of the HIPAA rules and regulations, as well as applicable federal and state laws.
- 3.1.5: Develop procedures to ensure each new member of the TDMHSAS workforce is trained on HIPAA privacy rules, policies and procedures, and document this training by requiring each trainee to sign a statement certifying he or she received privacy training. Work with the RMHI Privacy Officers to ensure such training is completed at the RMHIs.
- 3.1.6: Ensure appropriate administrative, technical, and physical safeguards are in place to ensure privacy of PHI, and to reasonably safeguard PHI from disclosures in violation of federal and state law.
- 3.1.7: Provide a process for individuals to make complaints, have complaints documented, ensure investigation and disposition of complaints, and ensure that any person seeking to file a complaint is not intimidated, coerced, threatened, or subjected to other retaliatory action.
- 3.1.8: Maintain working relationships with other state agencies and covered entities in the private sector concerning HIPAA issues.
- 3.1.9: To extent required by law, maintain contact with the U.S. Department of Health and Human Services, Office of Civil Rights (OCR) consistent with HIPAA rules and regulations, understand HIPAA audit requirements and methodologies, and report HIPAA violations as required by law.
- 3.1.10: Perform other responsibilities delineated in TDMHSAS HIPAA policies and procedures.
- 3.2: Duties of the RMHI Privacy Officers:
  - 3.2.1: Each RMHI Privacy Officer must ensure that all RMHI workforces are trained in HIPAA privacy regulations as well as TDMHSAS policies and procedures.
  - 3.2.2: Ensure appropriate administrative, technical, and physical safeguards are in place to ensure privacy of PHI, and to reasonably safeguard PHI from disclosures in violation of federal and state law.

3.2.3: When serving as the RMHI contact person, RMHI Privacy Officer must document and investigate complaints of HIPAA violations and work towards their resolution.

3.3: Duties of the TDMHSAS HIPAA Security Officer:

3.3.1: Assess and reduce risks and vulnerabilities to the security, confidentiality, integrity, and availability of electronic PHI that the TDMHSAS creates, receives, maintains, or transmits; and protect against reasonably anticipated threats to security.

3.3.2: Periodically review records of information security activity, such as audit logs, access reports, and security incident tracking reports.

3.3.3: Develop procedures to ensure that each new member of the TDMHSAS workforce is trained on HIPAA security rules, policies and procedures, and document this training by requiring each trainee to sign a statement certifying that he or she received security training.

3.3.4: Implement procedures to guard against, report, and detect malicious software.

3.3.5: Create log-in procedures for computer workstation security including monitoring log-in discrepancies, safeguarding passwords, responding to and documenting security incidents.

3.3.6: Ensure that all TDMHSAS workforce members have appropriate access to electronic PHI, including preventing those who should not have access from obtaining access. Implement procedures for terminating access to PHI stored electronically when a member of the TDMHSAS workforce terminates his or her employment, and require appropriate sanctions against workforce members who fail to comply with security policies and procedures.

3.3.6: Ensure that all HIPAA privacy policies are accessible to all TDMHSAS employees and available to the general public via internet access through the TDMHSAS website.

3.3.7: Establish a contingency plan for responding to an emergency or other occurrence, including a data backup plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures, and applications and data criticality analysis data used to assess sensitivity, vulnerability, and security of key information assets.

- 3.3.8: Provide assistance and guidance to RMHI Security Officers and department personnel as needed.
- 3.3.9: Maintain working relationships with other state agencies and covered entities in private sector concerning HIPAA security issues.
- 3.3.10: Perform other responsibilities delineated in TDMHSAS HIPAA policies and procedures.

3.4: Duties of the RMHI Security Officer

- 3.4.1: Each RMHI Security Officer must ensure that EMHI workforce is trained in HIPAA security rules, policies, and procedures, as well as related TDMHSAS policies and procedures.
- 3.4.2: Ensure that all workforce members have appropriate access to electronic PHI, including preventing those who should not have access from obtaining access. Implement procedures for terminating access to PHI stored electronically when a member of the TDMHSAS workforce terminates his or her employment.
- 3.4.3: Periodically review records of information system activity such as audit logs, access reports, and security independent tracking reports.
- 3.4.4: Perform other responsibilities delineated in the TDMHSAS HIPAA policies and procedures, and ensure any RMHI-specific policies and procedures related to HIPAA conform to TDMHSAS policies and procedures, as well as State and Federal law.

4. **Other Considerations:**

4.1: Authority

45 C.F.R. §164.308(a); 45 C.F.R. §164.530(a); 45 C.F.R. §164.530(b); 45 C.F.R. §164.530(i); 65 Fed. Reg. 82561 (Dec. 28, 2000)

Approved:

  
Commissioner

1-11-18  
Date